0.1 THE PLAN OF THE BOOK

The plan of this history appears in detail in the following Table of Contents: but a few general and preliminary remarks may be useful to the intending reader.

The first section after the Table of Contents is a general introduction, a sketch of the whole history of Hut 6, from the pen of the Head of the Hut, P.S. Milner-Barry. This account should certainly be read before the rest of the book is tackled as it gives a delightfully vivid bird's-eye view of Hut 6 and its life. It is true that it contains some technical terms which may puzzle a reader who comes to the History with no previous knowledge of the subject, but the general lines of the story are clear, and any obscure details are best left to be clarified by a second reading when the reader has delved further into the history.

After this introduction the history proper begins. Most of the main divisions or "Books" correspond to the chief functional divisions of Hut 6 and indeed are such as are almost inevitable in any cryptographic organisation. Traffic must be intercepted, then identified, then registered, then broken and then decoded; each of these operations was performed by a separate section of Hut 6 and to each a separate Book is devoted. The order given above (which is the normal chronological order) has been followed except that for obvious reasons breaking the traffic - the end of the whole process - has been placed first. It now remains to discuss the arrangement of the work within the various Books.

Book 1, CRYPTOGRAPHY, deals with the actual breaking of keys and with the work of the cryptographic sections - i.e. Watch, Research and Machine Room. The treatment throughout is primarily historical: after an introductory description of the machine five chapters follow on the main cryptographic periods of the war. Then two shorter chapters deal with the closely related subjects of Bombe Control and the History of the Machine Room: and finally we have a long chapter on the History of Special Groups of Keys and a short final one of General Comments on cipher security.

Technical details and full descriptions of the processes involved have not been inserted in this history - these will be found in the separately published "History of E/Breaking, Part II". There were three main reasons for taking this course.

(1) Even as matters stand, the Book on Cryptography is the largest division of this work, and if full technical details had been added the Book would have reached too disproportionate a length.

(2) It was believed that there would be considerable gain to clarity of exposition if the technical and historical approaches to cryptography were firmly separated and dealt with in separate works. To deal with them in the same book would have meant that confusing changes of standpoint would have occurred rather frequently.

(3) Technically, the problems of Hut 6 were similar in many respects to those of Hut 8. It was possible to bring this out (as has been done) in a joint Technical History but the problems of Hut 8 could clearly find no place in the history of Hut 6.

The result of the course taken is that the treatment of cryptography in the present work is as little technical as possible (with a few exceptions to be later mentioned). This history is, in short, written for the layman who should consult

the Technical History for further details on any point that has aroused his curiosity. On the other hand, the professional cryptographer may well prefer to read the Technical History first, and consult the present work later for the purpose of filling out the historical background.

The exceptions previously referred to are Chapters 1·0 and 1·1. These do contain a certain amount of technical detail and in fact Chapter 1·0 (which contains the unavoidable minimum of information about the machine) is taken direct from the Technical History. Chapter 1·1 deals with the early history of Hut 6 with which questions of technique are so closely bound up as to make impossible the rigid separation that is later enforced.

The only other comment worth making on Book 1 is that the constantly increasing complexity of the general cryptographic situation is reflected in the increasing length of the historical chapters. The stage was indeed crowded for the Fifth Act.

Book 2, INTERCEPTION, is much simpler in structure. The more technical side will be dealt with in other histories and we have only striven to deal with the matter from the Hut 6 point of view. After a general introduction and a chapter on Stations and Communications, there follows a chapter on the routines and history of the Control Room, the Hut 6 section concerned with interception. This central chapter is followed by a shorter one on the rather special subject of Overseas Interception, a few General Comments and a brief Appendix on Hut 6 Liaison with W.O.Y.G. For statistics of sets the reader is referred to the Statistical Appendix at the end of the whole work. It will be noticed that this Book is arranged by subject, and not, in the first instance, chronologically.

Book 3, TRAFFIC IDENTIFICATION, is apart from Book 1, the longest. Its special peculiarity is that it deals almost wholly with the period from November 1943 onwards when Traffic Identification first became a problem and T.I.S. was set up. Again the Book is arranged primarily by subject after a general introduction. The principle has been to describe in the first instance the normal routine of Initial Sorting and the work of the Duddery, then to discuss the more specialised work of Sector Investigation, first on the Air and then on the Army, with illustrations from specific sectors, and then to deal with the two great Traffic Identification crises in some detail. There is thus a steady progression from the simple to the complex. The final chapter 3·9 is in the nature of an Appendix containing a number of papers on special points, some of which are mainly intended for purposes of reference.

The remaining Books are very much shorter and, for that reason alone, have a clearer outline. In Registration and Decoding an attempt has been made to keep the basic routine quite separate from the refinements introduced to meet special problems and circumstances. The Statistical Appendix and Glossary are naturally mainly designed for reference.

It should perhaps be emphasised that the Books are to a great extent independent and though the order adopted seemed to us the best there is no very cogent reason why the reader should not pick and choose among the Books to suit his taste. But it is certainly advisable to read through in order whichever Book is chosen.

V

0·2 TABLE OF CONTENTS: VOLUME I

I

TABLE OF CONTENTS : VOLUME II

TABLE OF CONTENTS: VOLUME III